BGP MPLS VPN

- Mariem Zekri



Contexte

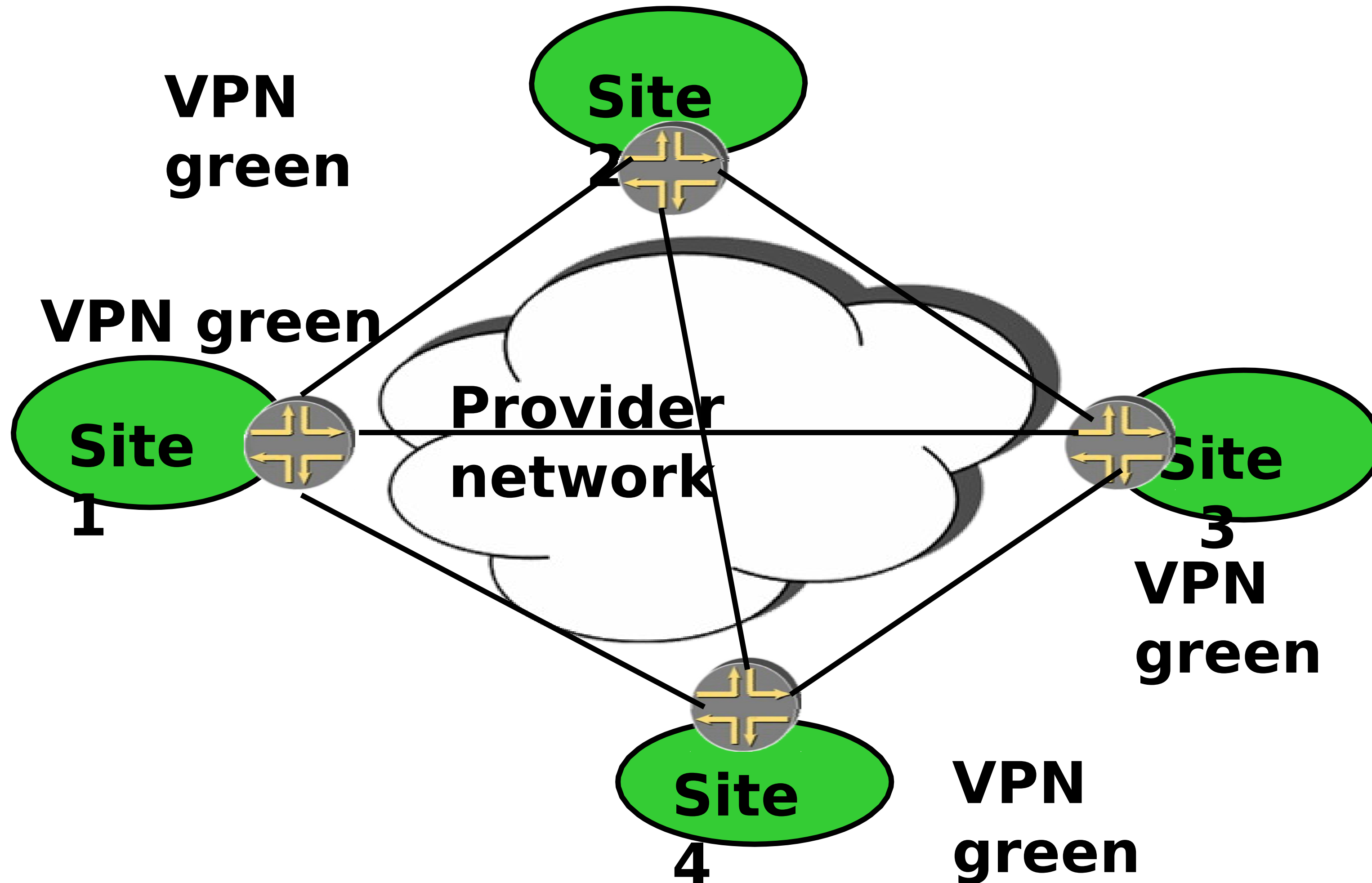
- Réseaux privés virtuels - fournissent un réseau privé sur une infrastructure partagée.
- Interconnectent des sites géographiquement séparés, avec la même confidentialité et les mêmes garanties qu'un réseau privé.

Le modèle « overlay »

- Réaliser un VPN *overlay* consiste à relier les sites clients par des circuits virtuels permanents.
- Les relations sont du type point à point.
- Si l'approche théorique de ce modèle est simple, la réalisation de réseaux VPN *overlay* est relativement complexe.
- Il faut définir avec précision les relations entre sites et créer autant de circuits virtuels que de relations point à point à émuler.
- Le nombre de circuits à définir croît avec le carré du nombre de sites ($N\,[N-1]/2$).
- Compte tenu du nombre de circuits à définir, les réseaux VPN *overlay* réalisent rarement un maillage complet.



Le modèle « overlay »



VPN MPLS- Modèle Peer

Objectif: résoudre les problèmes de mise à l'échelle. Prend en charge des milliers de VPN, prend en charge les VPN avec des centaines de sites par VPN, prend en charge les espaces d'adressage qui se chevauchent.

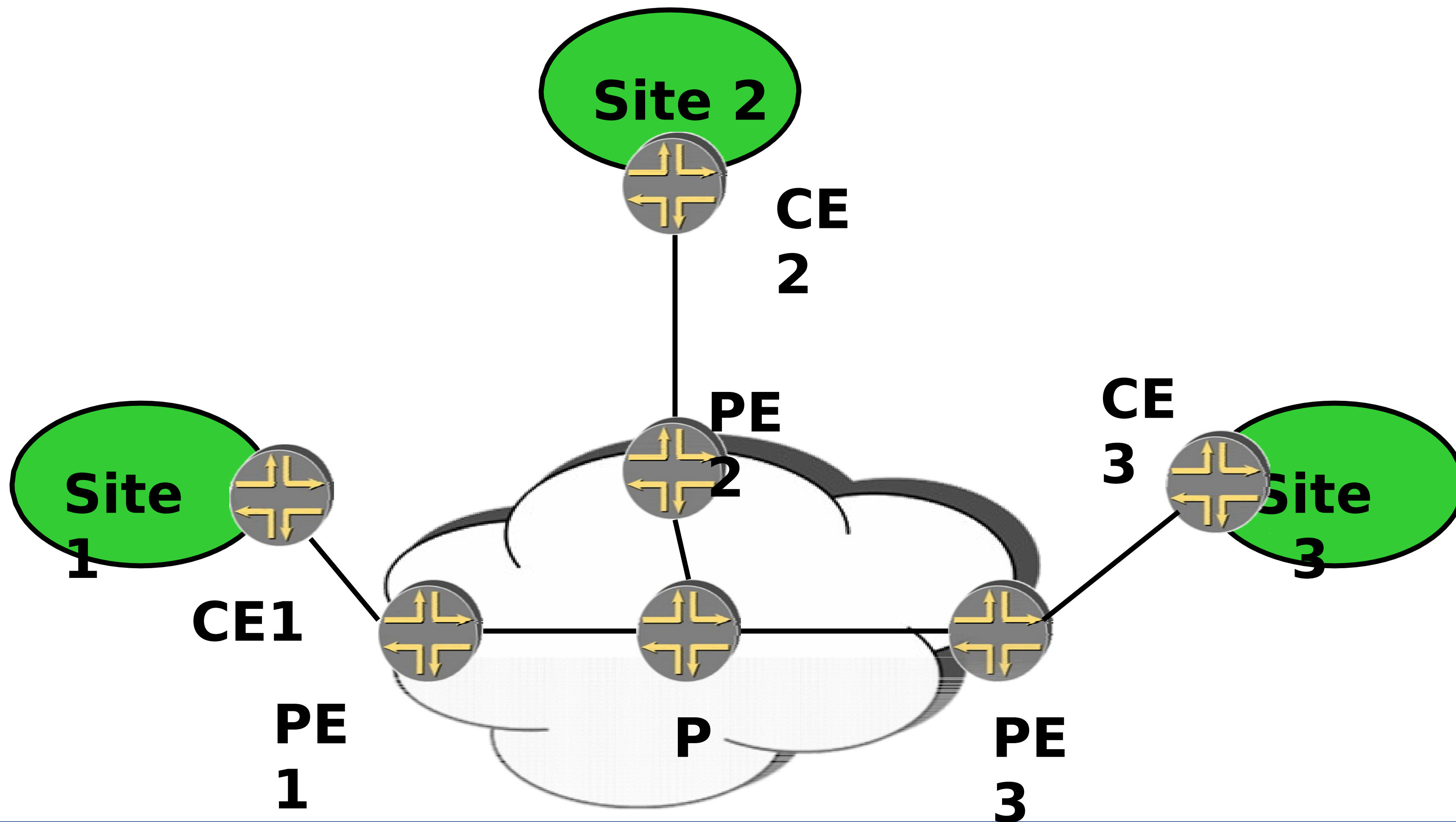
➔Modèle homologue ou peer

- Les VPN sont ignorés du cœur de réseau
- Les données échangées entre les clients d’un même VPN sont acheminées dans le réseau comme des données ordinaires.
- Les routeurs de cœur de réseau n’ont plus de nombreux circuits virtuels à gérer et l’ajout d’un client n’a aucun impact sur le réseau.

Terminologie

- 3 types de routeurs : P, PE, CE
- Router « P » (*Provider*) : appartient au cœur de réseau de l'opérateur, il n'a aucune notion de VPN (pas de connexion de clients)
- Router « PE » (*Provider Edge*): appartient à l'opérateur, ces routeurs raccordent les clients au fournisseur de service.
- Routeur « CE » (*Customer Edge*): appartient au client, et n'a aucune notion de MPLS.
- Les routeurs « P » ne sont pas obligatoires, il est tout à fait possible de monter un backbone avec uniquement des routeurs PE.

VPN MPLS- Modèle Peer



Proprietés du modèle

- Le routeur CE est peer avec un routeur PE, mais pas avec d'autres routeurs CE.

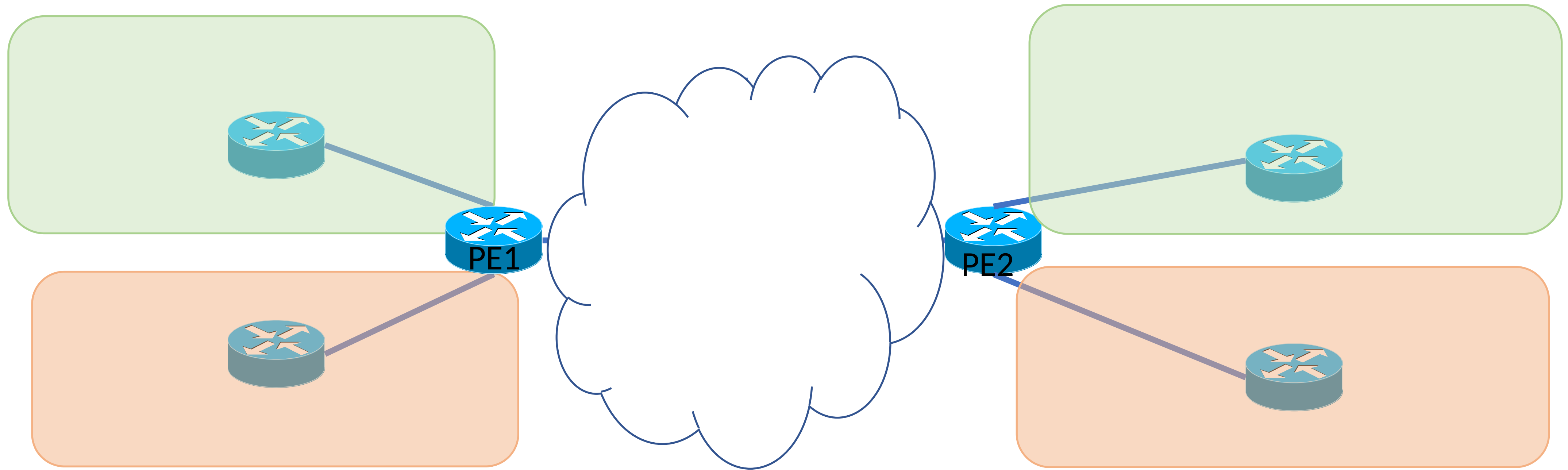
- L'ajout / la suppression d'un nouveau site nécessite la configuration du routeur PE connecté au site.

- Un routeur PE a uniquement besoin de maintenir des routes pour les VPN dont les sites sont directement connectés à lui.

Objectif

- Obtenir une connectivité intersites
- Confidentialité - ne pas autoriser le trafic d'un VPN à être vu dans un autre VPN
- Adressage indépendant - adresses privées dans chaque VPN.

Distribution des informations de Routage



Principes du VPN MPLS

- Séparation du forwording
- Nouveau type d'adresse
- Distribution des informations de routage
- Transfert avec MPLS

Séparation du forwording

- Objectif: contrôler la connectivité et garantir la confidentialité en séparant les informations de transfert.

- Routeur PE connecté à des CE appartenant à plusieurs VPN.

- Avec une seule table de forwording, il est possible de transférer des paquets d'un VPN à un autre.

Plusieurs tables de forwording

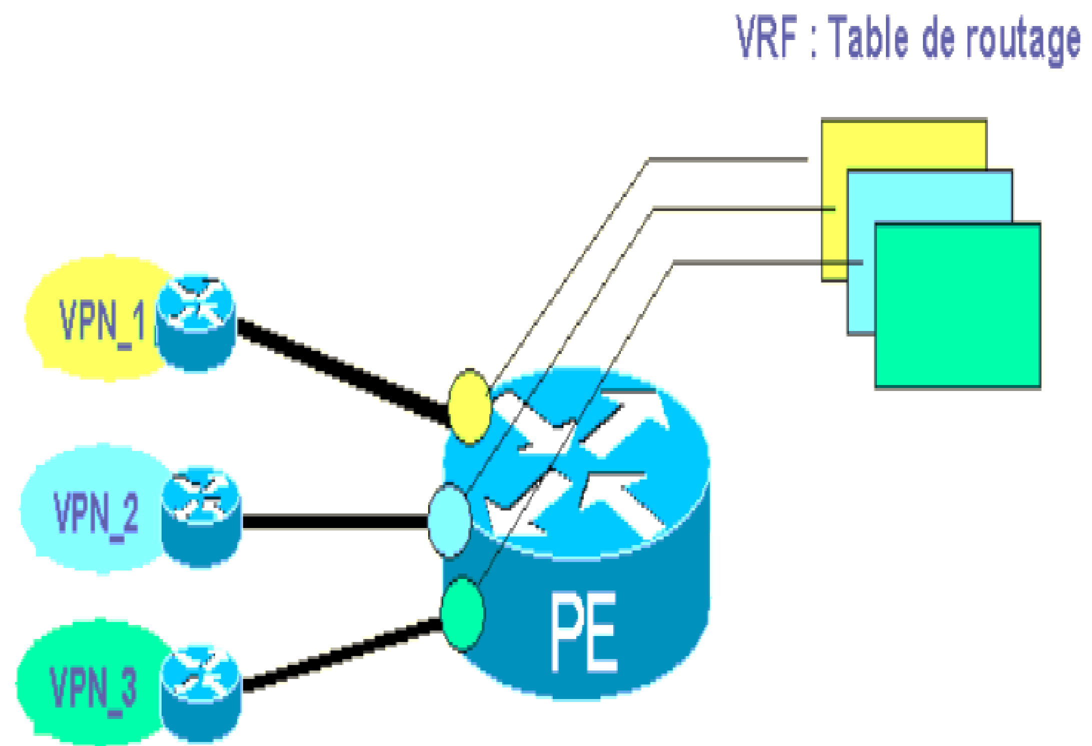
- Plusieurs tables de forwording - chaque table associée à un site.
- Les paquets du client sont identifiés en fonction du port entrant, qui identifie la table de transfert.
- Contenu: routes reçues du CE et routes reçues des PE distants.

- Table de routage et de transfert VPN appelée - VRF.

VRF

- La VRF contient la désignation du PE, auquel sont rattachés le client VPN destinataire, la classe d’équivalence associée (**FEC**, *Forwarding Equivalence Class*) et le label identifiant le VPN d’appartenance.
- La VRF contient ainsi tous les éléments d’acheminement, y compris une copie dédiée de la LFIB.
- Une VRF correspond à un routeur dédié au VPN (**routeur virtuel**).

VRF

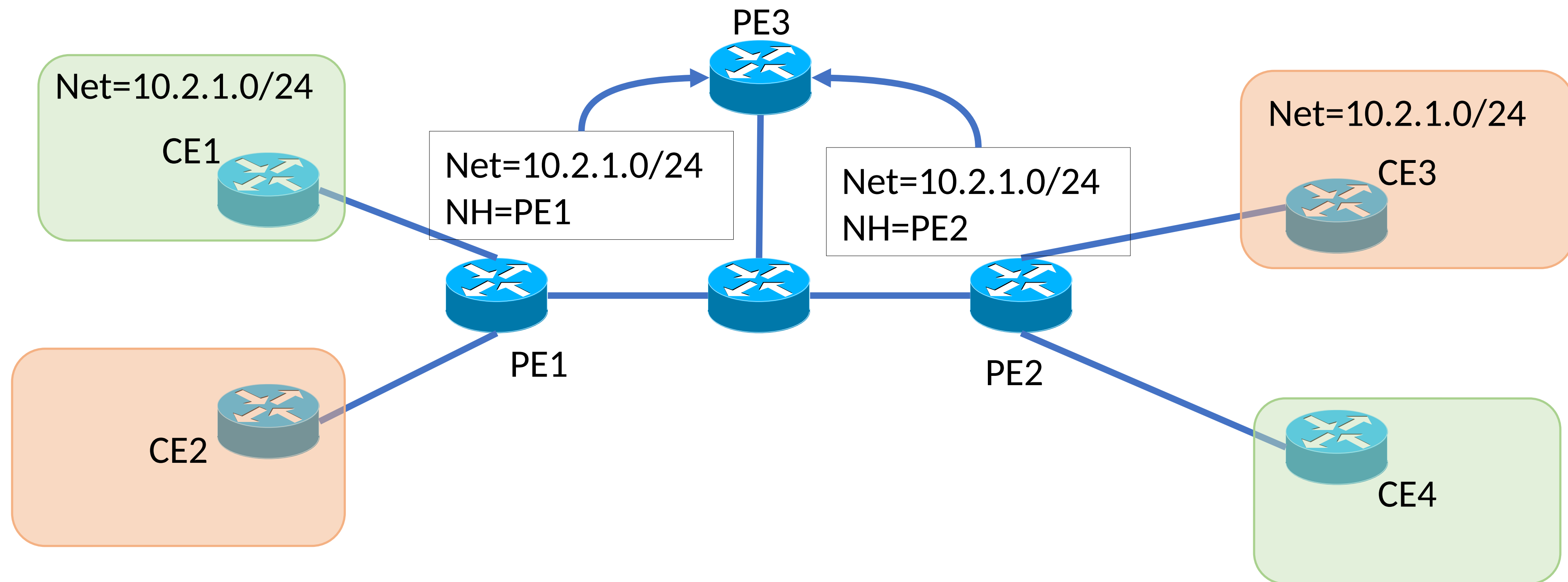


Adresses VPN-IP

- Les clients utilisent des espaces d'adressage qui se chevauchent.

Comment résoudre le problème d'unicité des adresses?

Visualiser le problème



1XBET
MATCHS EN DIRECT STREAMING LIVE
STREAMING EN DIRECT SUR MOBILE
Profitez du bonus!

Inscription
Par téléphone

Code *
+7
Téléphone *
912 676-78-48

Devise *
Dollar américain (USD)

Code promo (facultatif)
1SYSCASHBACK

Bonus
Bonus pour le sport

Conditions générales

Politique de confidentialité

J'ai plus de 18 ans et je confirme avoir lu et accepté les conditions générales et la politique de confidentialité de la société.

J'accepte de recevoir des offres marketing et promotionnelles par téléphone

S'inscrire

PROFESSIONAL 61% 15:31

1XBET PRO
49.77 • 1X PRO

Pro Hub | Sports | Esports | Casino | 1xGames

PRIORITY AVANT-MATCH Sport Tout

Matchs amicaux. Équipes nationales Soon
Croatie Belgique
00 : 28 : 50
02.06.2026 (16:00)
1X2

V1 2.28	X 2.71	V2 2.256

TOURNOIS EN DIRECT Sport Tout

Hot Irak. Stars League 6
Hot Russie. Coupe SFD-NCFD 1
Hot Cuba. Liga de Barrios 1

RECOMMANDÉES Casino Tout

Pro Hub | Market Analysis | Slip Mgr. | Performance | Account

Inscription
Par e-mail

E-mail *
xxxxxxxxxxx@gmail.com

Code
+7
Téléphone
000 000-00-00

Mot de passe *
WrlnPassword14

Répéter mot de passe *
WrlnPassword14

Exigences du mot de passe

Code promo (facultatif)
1SYSCASHBACK

Bonus
Bonus pour le sport

S'inscrire

1XBET
Bonus de 200 % sur le premier dépôt
Jeu responsable. Termes & conditions appliqués. 18+
Profitez du bonus!

MEGABONUS POUR LE PREMIER DÉPÔT
PACK DE BIENVENUE JUSQU'À 1500 € + 150 TOURS GRATUITS
INSCRIPTION

Adresses VPN-IP

- Objectif: transformer les adresses non uniques en adresses uniques adresse VPNv4

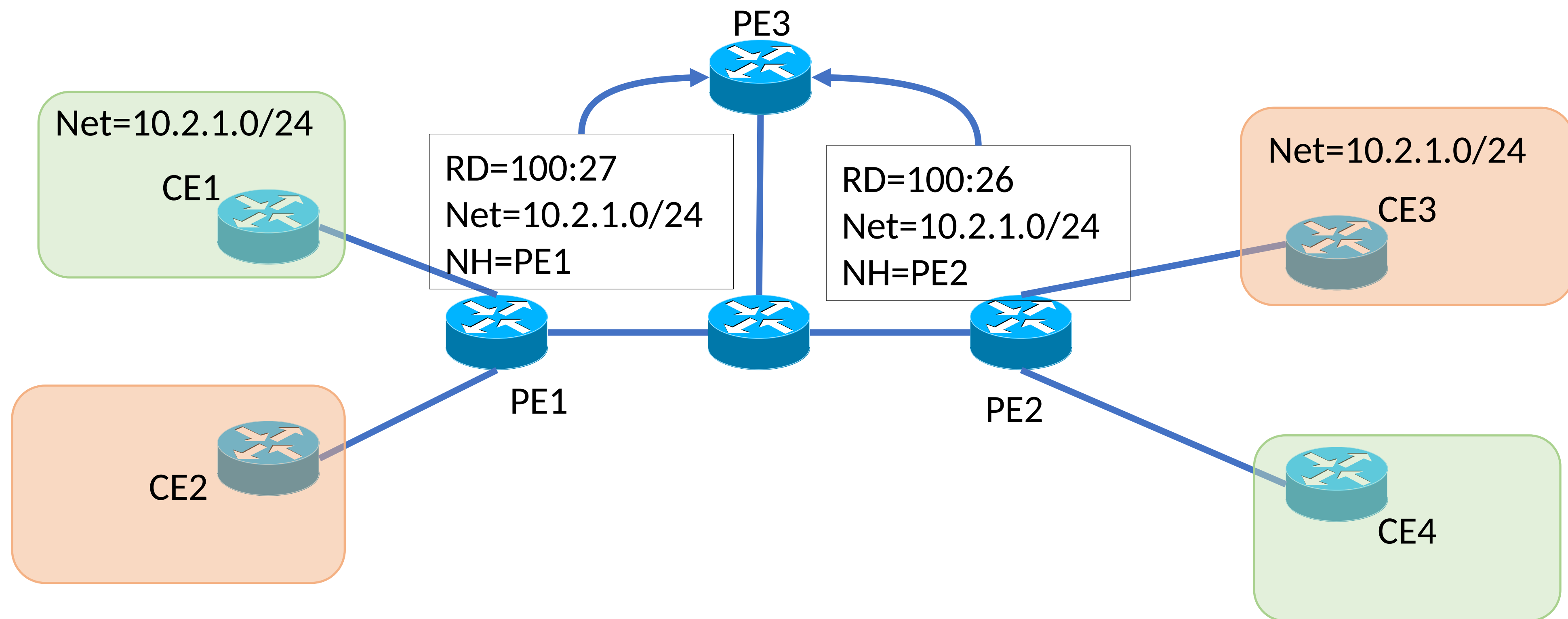
- Les routes échangées contiennent notamment un préfixe dit « VPN-IPv4 » (Préfixe IPv4 + Route Distinguisher) et un Label MPLS, local au PE qui fait l’annonce.

- Le RD (*Route Distinguisher*) permet de distinguer les routes de clients différents. Le RD a une taille de 8 octets (il est configuré manuellement par l’opérateur).

Adresses VPN-IP

- Utilisé uniquement sur le réseau du fournisseur.
- Utilisé uniquement dans le plan de contrôle.
- La traduction d'adresses IP en adresses IP VPN se produit sur le PE.
- Non utilisé pour le filtrage des itinéraires (nous utilisons des communautés pour cela).

Adresses VPN-IP



Route Target

Un lecteur attentif peut commencer à poser une question intéressante: comment le routeur sait-il quelles routes doivent être insérées dans quel VRF?

- Ce dilemme est résolu par l'introduction d'un autre concept dans l'architecture MPLS / VPN: la Route Target.
- Chaque route VPN est étiquetée avec une Route Target lorsqu'elle est exportée à partir d'un VRF (à offrir à d'autres VRF).
- Toutes les routes étiquetées avec une Route Target seront insérées dans le VRF qui lui correspond.
- REMARQUE: La Route Target est l'approximation la plus proche d'un identifiant VPN dans l’architecture MPLS / VPN
- REMARQUE: La Route Target est une quantité de 64 bits.
- Pour des raisons de simplicité, nous utiliserons des noms pour les Route Target dans ce chapitre.

Route Target

10.2/16 route-target green

Customer green

Site 2

10.2/16

CE 2

CE 4

Site 2

10.1/16

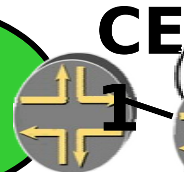
10.1/16 route-target gray

Customer gray

Customer green

Site 1

10.1/16



CE 1

CE 3

Site 1

10.2/16

10.1/16 route-target green

Customer gray

10.2/16 route-target gray

Propagation des informations de routage VPN dans le réseau

- CE annonce les routes vers le PE local via un protocole.
- Le PE local marque ces routes avec une Route Target et les annonce.
- Le PE distant reçoit les routes, les filtre en fonction de la communauté et les annonce au CE.

Mais quels protocoles utiliser?

BGP

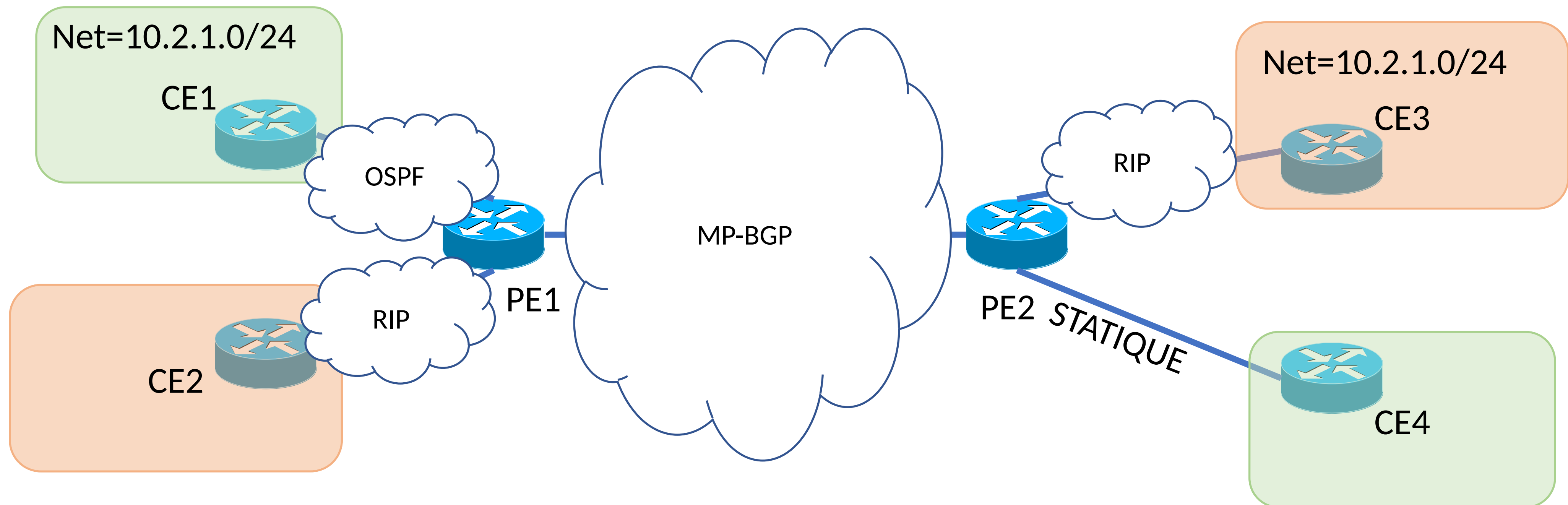
Raisons de choisir BGP pour transporter les routes VPN:

- Le nombre de routes VPN dans un réseau peut devenir très important.
- BGP est le seul protocole de routage pouvant prendre en charge un très grand nombre de routes et des familles d'adresses différentes.
- BGP est également conçu pour échanger des informations entre des routeurs qui ne sont pas directement lié.
- Cette fonctionnalité BGP prend en charge la conservation des informations de routage VPN hors des routeurs principaux du fournisseur (routeurs P).

MP-BGP

- BGP supporte à la base uniquement les adresses IPv4.
- Evolution vers MP-BGP
- Les adresses VPNv4 de 96 bits résultantes sont échangées entre les routeurs PE en utilisant le Multiprotocol BGP (désignée ici par MP-BGP).

Distribution des informations de Routage



Distribution des informations de Routage

Etape 1:

- Le routeur PE1 collecte les informations de routage du site CE 1 à l'aide d'un processus OSPF. De même, les informations du site CE2 sont collectées à l'aide d'un processus RIP.

Etape 2:

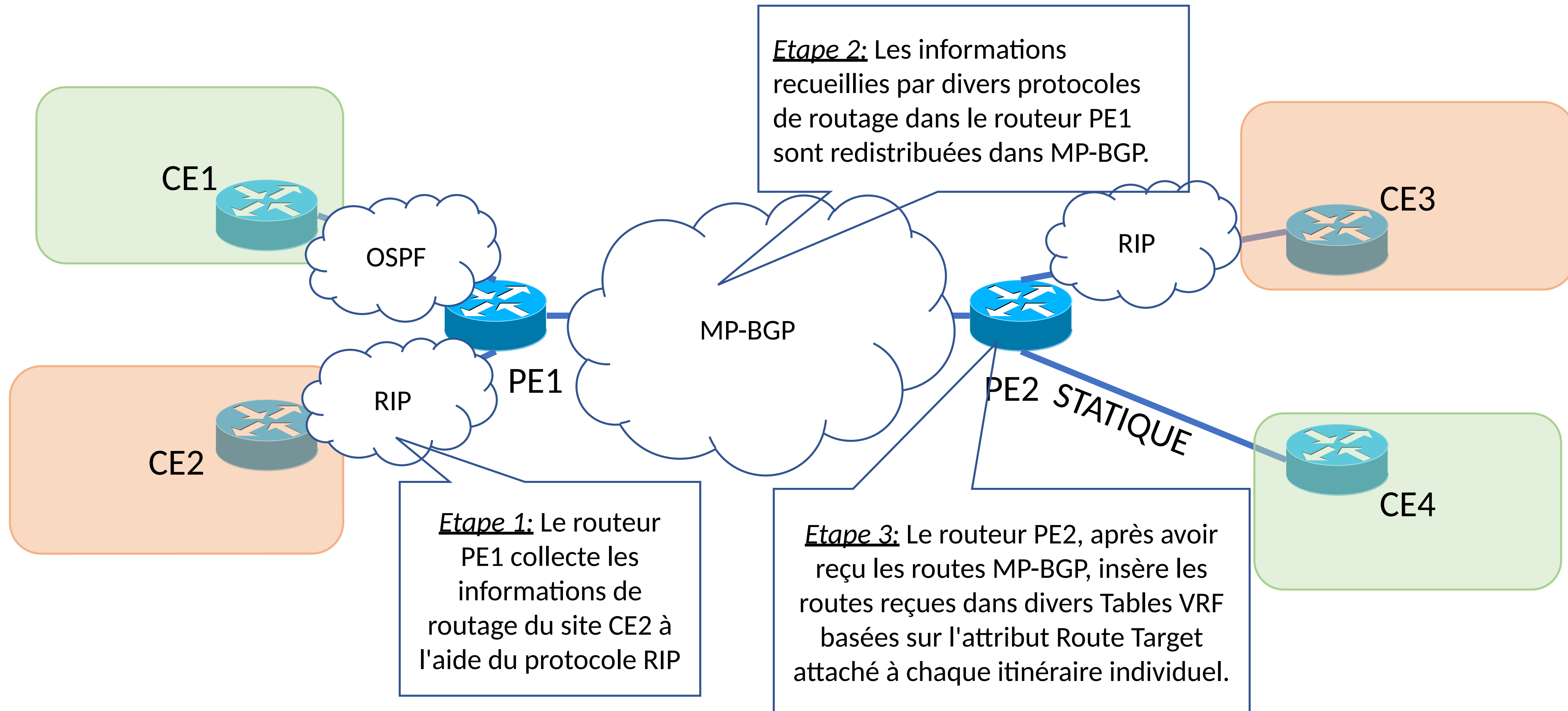
- Les informations recueillies par divers protocoles de routage dans le routeur PE1 sont redistribuées dans MP-BGP.
- Les adresses sont augmentées des RD au moment de la redistribution.
- La route target d'exportation de route spécifiée dans le VRF d'origine est également attachée à la route.
- Les informations de routage 96 bits résultantes sont propagées par MP-BGP au routeur de PE2.

Distribution des informations de Routage

Etape 3:

- Le routeur de PE2, après avoir reçu les routes MP-BGP, insère les routes reçues dans divers Tables VRF basées sur l'attribut Route Target attaché à chaque itinéraire individuel.
- Le RD est supprimé de la route lorsque la route est insérée dans le VRF, résultant encore une fois dans une route IP traditionnelle.
- Enfin, les informations de routage reçues via BGP est redistribué dans le processus RIP et transmis au site CE3 et CE4.

Distribution des informations de Routage



Et la commutation?

- Toutes les informations de routages sont disponibles!
- Comment transférer un paquet à travers le cœurs MPLS sans avoir à aller creuser dans l'entête du paquet ni avoir à apporter des modifications aux mécanismes traditionnels?

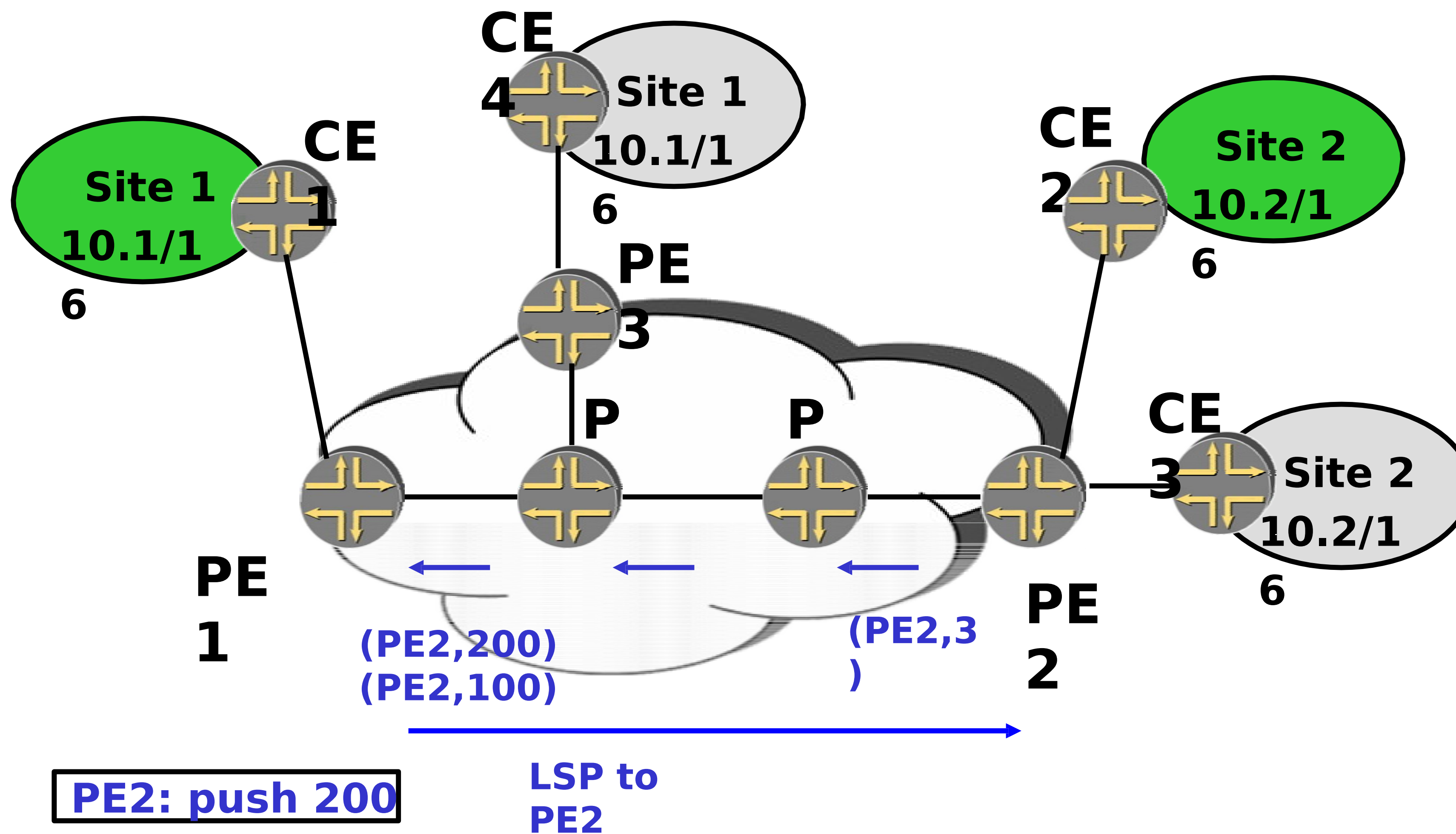


Commutation VPN MPLS

<u>*Commutation dans le cœur*</u>

- Le paquet est étiqueté par le routeur PE d'entrée avec une étiquette identifiant de manière unique le routeur PE de sortie et est envoyé sur le réseau.
- Tous les routeurs du réseau commutent ensuite le paquet en se basant sur le label sans avoir à regarder dans le paquet lui-même.
- Chaque routeur PE a besoin d'un identifiant unique (généralement l'adresse IP de bouclage est utilisé), qui est ensuite propagé dans tout le réseau P en utilisant l'IGP habituel.
- Une étiquette est attribuée dans chaque P-routeur pour cette route d'hôte et est propagée à chacun de ses voisins.
- Enfin, tous les autres routeurs PE reçoivent une étiquette associée au routeur PE de sortie via un processus de distribution d'étiquettes MPLS (LDP).

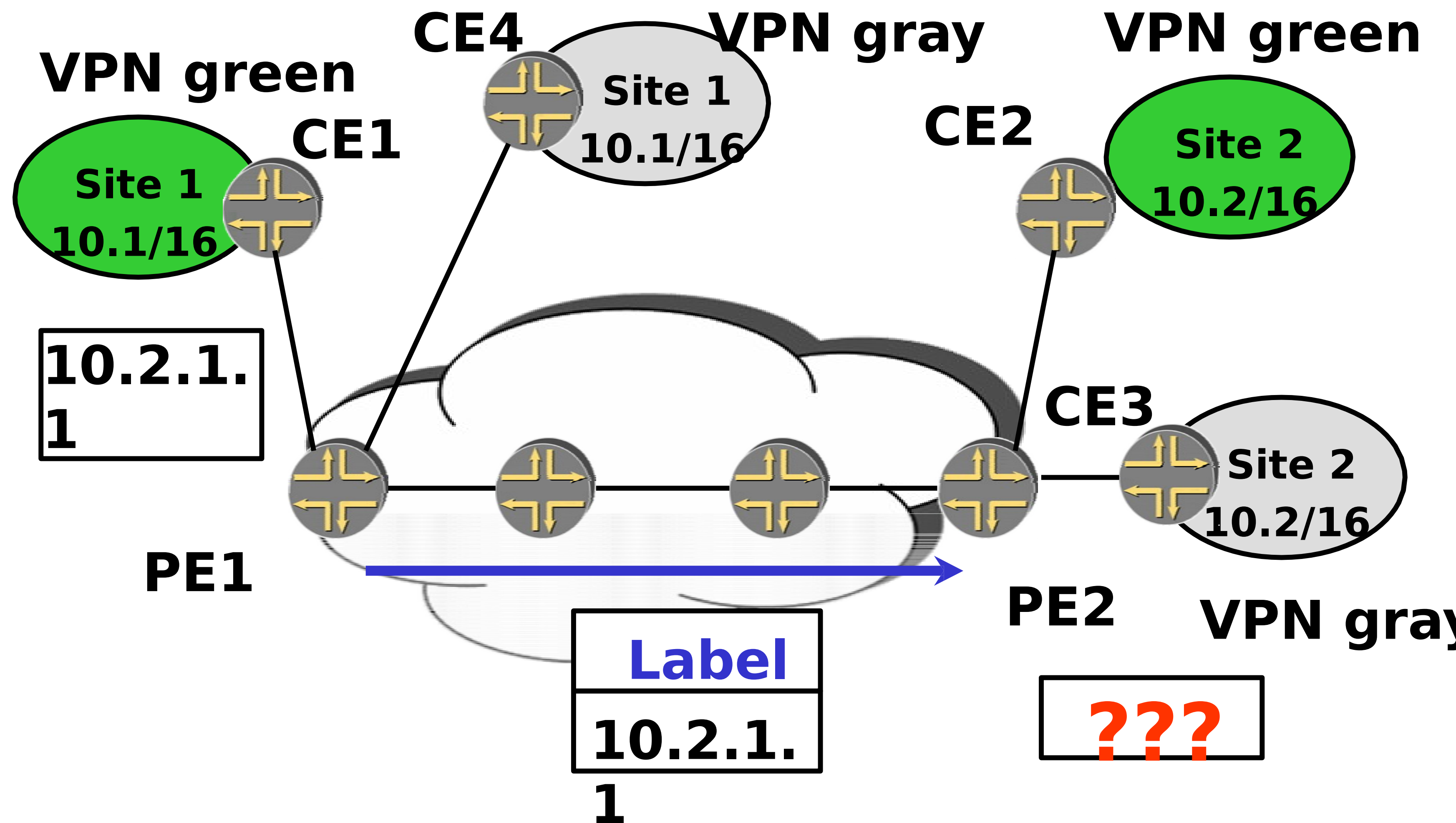
Commutation dans le cœur



Traffic → ← Forwarding info

Commutation dans le cœur

Lorsque le routeur PE de sortie reçoit le paquet VPN, il n'a aucune information pour lui dire à quel VPN le paquet est destiné.

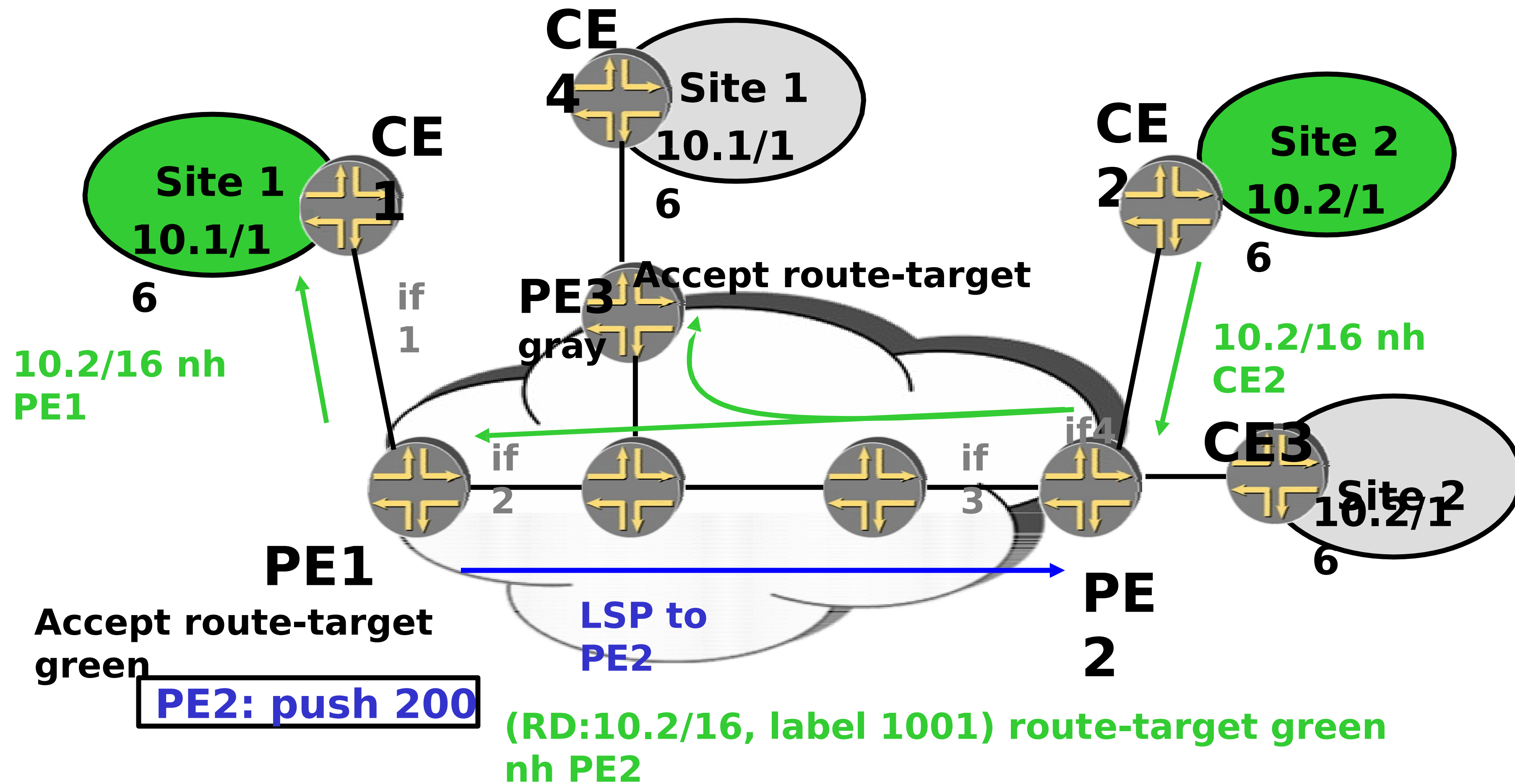


Commutation VPN MPLS

Identification du VPN

- Pour rendre la communication entre les sites VPN unique, un deuxième ensemble d'étiquettes est introduit.
- Chaque PE-routeur attribue une étiquette unique pour chaque route dans chaque instance de routage et de transfert VPN (VRF).
- Ces étiquettes sont propagées avec les routes correspondantes via MP-BGP vers tous les autres routeurs PE.
- Lorsqu'un paquet VPN est reçu par le routeur PE d'entrée, le VRF correspondant est examiné, et l'étiquette associée à l'adresse de destination par le routeur PE de sortie est extraite.

Identification du VPN

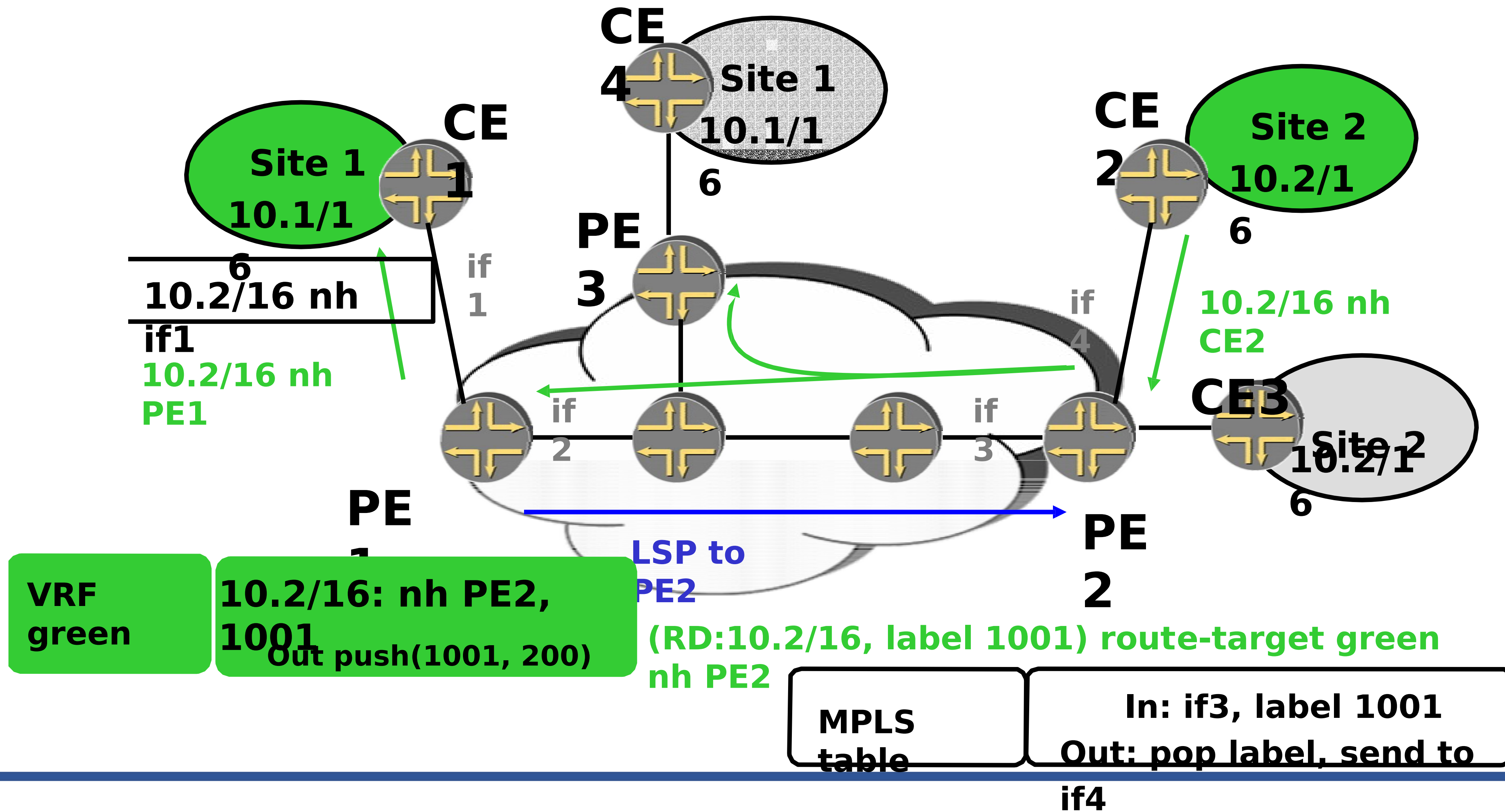


Traffic → ← Routing info

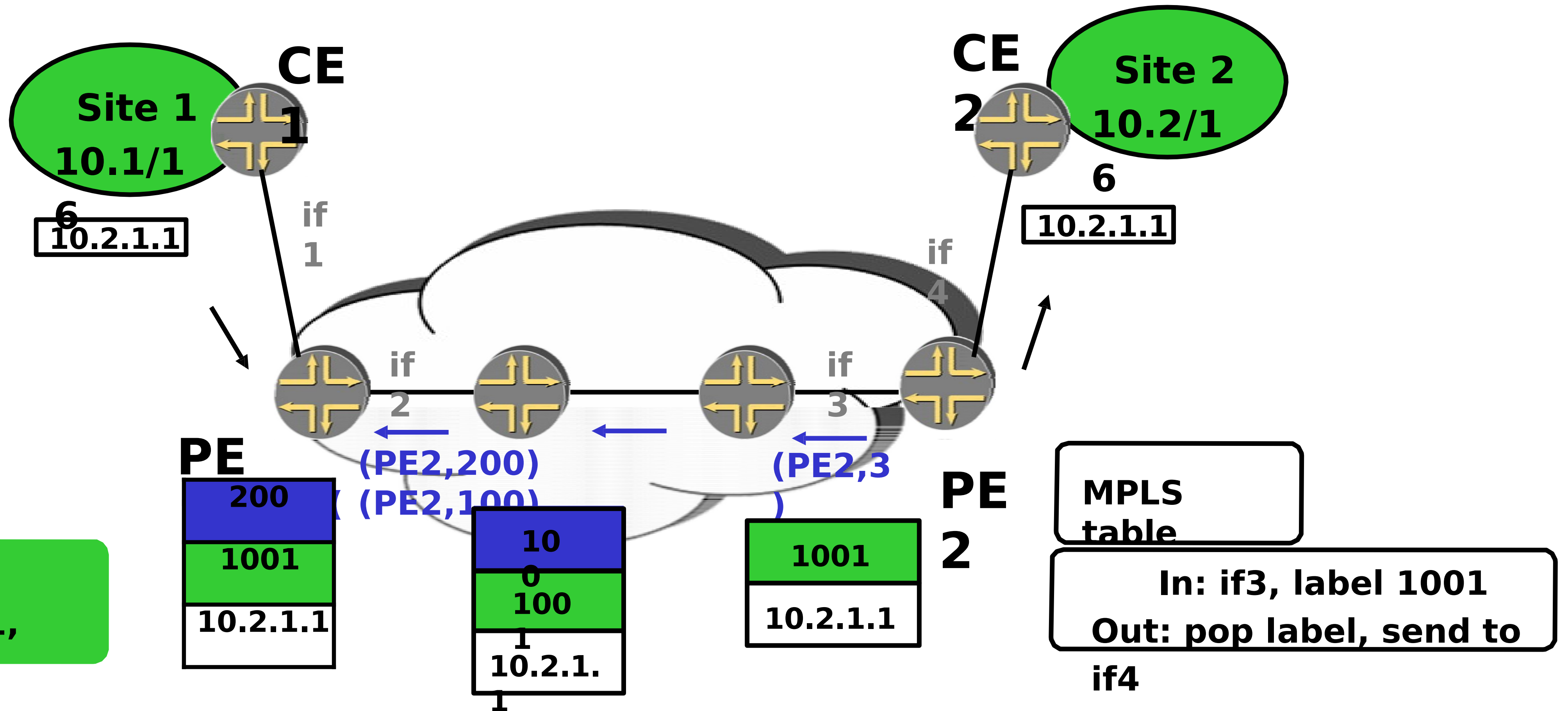
Commutation VPN MPLS

- Les deux étiquettes sont combinées dans une pile d'étiquettes MPLS, sont attachées devant le paquet VPN et sont envoyées vers le routeur PE de sortie.
- Tous les P-routeurs du réseau commutent le paquet VPN en se basant uniquement sur l'étiquette supérieure de la pile, qui pointe vers le routeur PE de sortie. Les P-routeurs ne regardent jamais au-delà de la première étiquette et sont donc complètement ignorants de la seconde étiquette ou du paquet VPN transporté à travers le réseau.

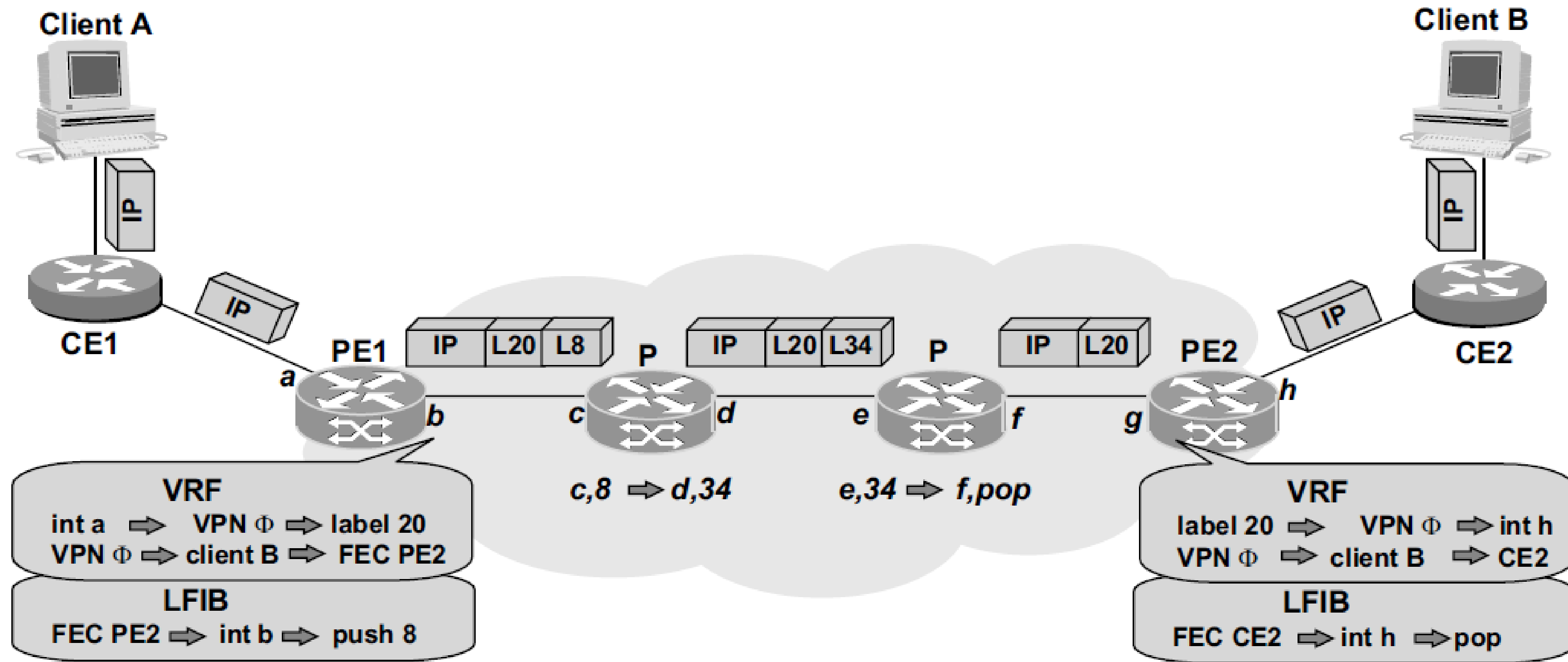
Commutation VPN MPLS



Commutation VPN MPLS

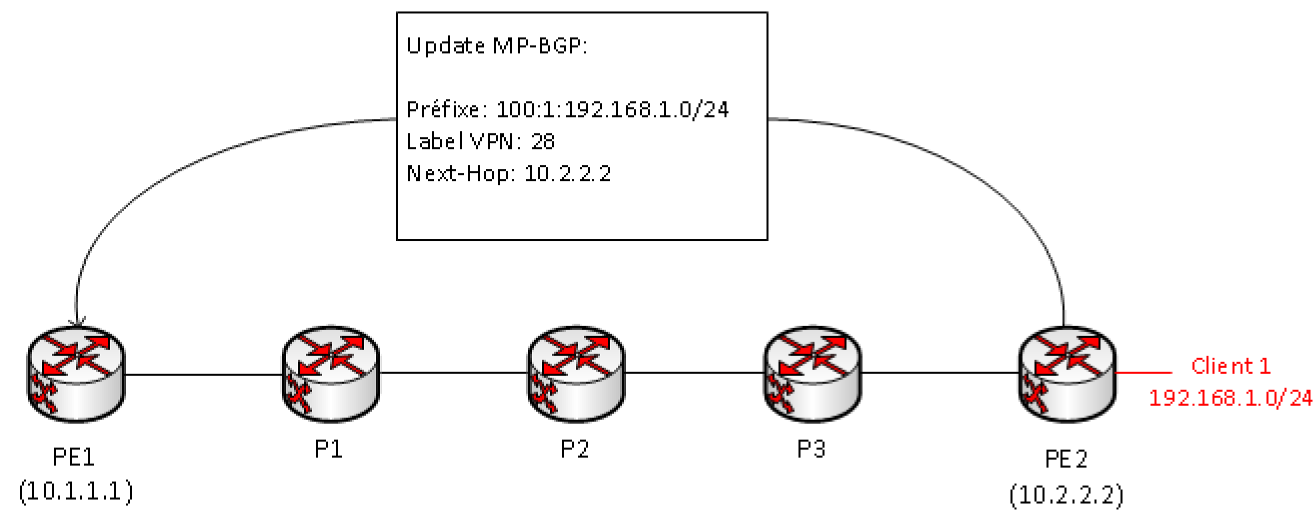


VRF

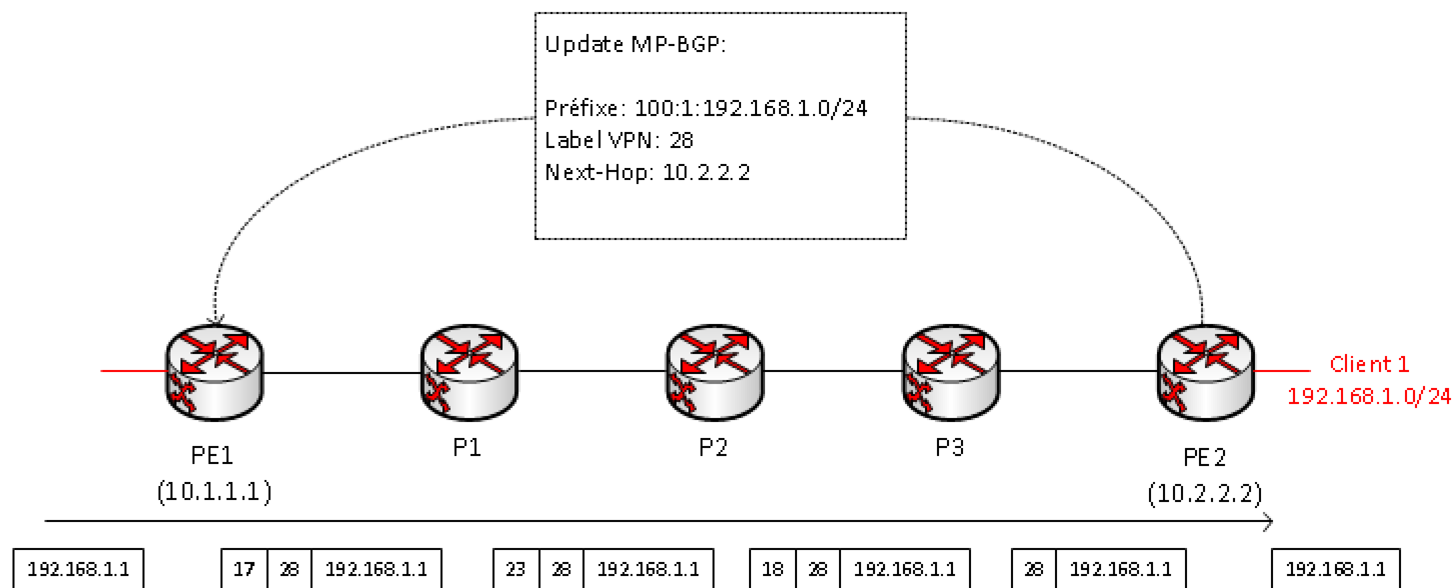


Client A
Client B
IP
IP
CE1
CE2
IP
IP
PE1
P
P
PE2
IP L20 L8
IP L20 L34
IP L20
a
b
c
d
e
f
g
h
c,8 ⇨ d,34
e,34 ⇨ f,pop
VRF
int a ⇨ VPN Φ ⇨ label 20
VPN Φ ⇨ client B ⇨ FEC PE2
LFIB
FEC PE2 ⇨ int b ⇨ push 8
VRF
label 20 ⇨ VPN Φ ⇨ int h
VPN Φ ⇨ client B ⇨ CE2
LFIB
FEC CE2 ⇨ int h ⇨ pop

Application



Application



IPv6 Provider Edge

Principes de 6PE

- Raccordement de clients IPv6, à travers un cœur MPLS (RFC 4798)
- Pas de normalisation de LDP pour IPv6 => Utilisation de MP-BGP
- Avec 6PE, le cœur n’a pas besoin d’être « IPv6-aware »
- Avantages :
  - Ne nécessite pas un upgrade du cœur, on conserve l’existant
  - Seuls les routeurs PE doivent être mis à jour et supporter 6PE
- Même principe que pour VPNv4 => 2 labels sont utilisés, le 1er pour atteindre le PE de sortie, le 2nd correspondant au préfixe IPv6 sur le PE.
- Le Next-Hop BGP est annoncé sous forme d’adresse IPv6 « IPv4-Mapped ». Les PE extraient l’adresse IPv4 et recherchent le label annoncé par LDP pour cette adresse.

IPv6 Provider Edge

